

IFW AF

TRANSMITTAL OF APPEAL BRIEF (Large Entity)	Docket No. EN998146
---	-------------------------------

In Re Application Of: **Fetkovich et al.**

Application No. 09/443,204	Filing Date 11/18/1999	Examiner Santos Patrick J.D.	Customer No. 30400	Group Art Unit 2171	Confirmation No. 6903
--------------------------------------	----------------------------------	--	------------------------------	-------------------------------	---------------------------------

Invention: **DYNAMIC ENCRYPTION AND DECRYPTION OF A STREAM OF DATA**

COMMISSIONER FOR PATENTS:

Transmitted herewith in triplicate is the Appeal Brief in this application, with respect to the Notice of Appeal filed on **June 23, 2004**

The fee for filing this Appeal Brief is: **\$330.00**


- ☐ A check in the amount of the fee is enclosed.
- ☐ The Director has already been authorized to charge fees in this application to a Deposit Account.
- ☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **09-0457 (IBM)**


Signature

Kevin P. Radigan, Esq.
Registration No.: 31,789

HESLIN ROTHENBERG FARLEY & MESITI, P.C.
5 Columbia Circle
Albany, New York 12203
Tel: (518) 452-5600
Fax: (518) 452-5579

Dated: **August 23, 2004**

I certify that this document and fee is being deposited on August 23, 2004 with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
 Signature of Person Mailing Correspondence
Kevin P. Radigan Typed or Printed Name of Person Mailing Correspondence

CC:



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants: Fetkovich et al.

Group Art Unit: 2171

Serial No.: 09/443,204

Examiner: Santos Patrick J.D.


Filed: 11/18/99

Appeal No.:

For: DYNAMIC ENCRYPTION AND DECRYPTION OF A STREAM OF DATA

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on August 23, 2004.


Kevin P. Radigan
Attorney for Appellants
Registration No. 31,789

Date of Signature: August 23, 2004

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

08/26/2004 RMEBRAHT 00000013 090457 09443204

01 FC:1402 330.00 DA

Brief of Appellants

Dear Sir:

This is an appeal from a final rejection, dated March 23, 2004, rejecting claims 1, 2, 4, 5, 7-14, 16-19, 21-29, 31, 32, and 34-38, all the claims being considered in the above-identified application. This Brief is accompanied by a transmittal letter authorizing the charging of Appellants' deposit account for payment of the requisite fee set forth in 37 C.F.R. §1.17(c).

EN998146

Real Party In Interest

This application is assigned to **International Business Machines Corporation** by virtue of an assignment executed by the inventors on October 13, 1999; October 14, 1999; and November 15, 1999, and recorded with the United States Patent and Trademark Office at reel 010405, frame 0321, on November 18, 1999. Therefore, the real party in interest is **International Business Machines Corporation**.

Related Appeals and Interferences

To the knowledge of the Appellants, Appellants' undersigned legal representative, and the assignee, there are no other appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in the instant appeal.

Status of Claims

This patent application was filed on November 18, 1999, with the U.S. Patent and Trademark Office. As filed, the application included 38 claims, of which four (4) were independent claims (i.e., claims 1, 14, 27, & 28).

In an initial Office Action dated September 25, 2003, claims 1-26, 35 and 38 were rejected under 35 U.S.C. §112, second paragraph, as indefinite for failing to particularly point out and distinctly claim the subject matter regarded as the invention. Additionally, claims 1, 2, 5-8, 12-19, 26 and 27 were rejected under 35 U.S.C. §102(b) as anticipated by Jones (U.S. Patent No. 5,412,730; hereinafter "Jones"); claim 28 was rejected under 35 U.S.C. §102(b) as anticipated by Warren et al. (U.S. Patent No. 5,719,937; hereinafter "Warren"); and claims 1, 13, 14 and 26 were rejected under 35 U.S.C. §102(b) as anticipated by Aucsmith et al. (U.S. Patent No. 5,991,403; hereinafter "Aucsmith"). In addition, claims 3, 9-11, 20 and 22-25 were rejected under 35 U.S.C. §103(a) as unpatentable over Jones in view of Nardone et al. (U.S. Patent No. 5,805,700; hereinafter "Nardone") and in further view of Leppek (U.S. Patent No. 5,933,501; hereinafter "Leppek"); claims 4 and 21 were rejected under 35 U.S.C. §103(a) as unpatentable

EN998146

over Jones in view of Nardone and Leppek and in further view of an article entitled “Digital Television Achieves Maturity” by Leonardo Chiariglione (hereinafter “Chiariglione”); claims 29 and 32-35 were rejected under 35 U.S.C. §103(a) as unpatentable over Jones in view of Warren; claims 30 and 36-38 were rejected under 35 U.S.C. §103(a) as unpatentable over Jones, Nardone and Leppek in view of Warren; and claim 31 was rejected under 35 U.S.C. §103(a) as unpatentable over Jones, Nardone, Leppek, and Chiariglione in view of Warren. In Appellants’ response dated December 23, 2003, claims 1, 2, 4, 5, 7-14, 16-19, 21-29, 31, 32 & 34-38 were amended and claims 3, 6, 15, 20, 30 & 33 were cancelled (without prejudice).

In a final Office Action dated March 23, 2004, claims 1-3, 5-20 and 22-27 were rejected under 35 U.S.C. §103(a) as unpatentable over Jones in view of Nardone and further in view of Leppek; claims 1, 13, 14 and 26 were rejected under 35 U.S.C. §103(a) as unpatentable over Aucsmith in view of Nardone and Leppek; claims 4 and 21 were rejected under 35 U.S.C. §103(a) as unpatentable over Jones in view of Nardone and Leppek, and further in view of Chiariglione; claim 28 was rejected under 35 U.S.C. §103(a) as unpatentable over Warren in view of Nardone, and further in view of Leppek; claims 29-30 and 32-38 were rejected under 35 U.S.C. §103(a) as unpatentable over Jones in view of Warren, further in view of Nardone and Leppek; and, claim 31 was rejected under 35 U.S.C. §103(a) as unpatentable over Jones, Nardone, Leppek and Chiariglione in view of Warren. In Appellants’ response dated May 17, 2004, no claims were amended.

As of the time of filing this Brief, Appellants have not received a reply from the Patent Office to their response dated May 17, 2004.

A Notice of Appeal to the Board of Patent Appeals and Interferences was filed on June 23, 2004. The status of the claims is therefore as follows:

Claims allowed – none;

Claims objected to – none;

Claims rejected – 1, 2, 4, 5, 7-14, 16-19, 21-29, 31, 32 & 34-38; and

Claims canceled – 3, 6, 15, 20, 30 & 33.

Appellants are appealing the rejection of claims 1, 2, 4, 5, 7-14, 16-19, 21-29, 31, 32, and 34-38.

Status of Amendments

Appellants proffered no amendments responsive to the final Office Action dated March 23, 2004. The claims as set out in the Appendix include all prior entered claim amendments.

Summary of the Invention

Appellants' disclose a technique (e.g., claims 1, 14, 27, 28) for protecting a stream of data to be transferred between an encryption unit 20 (FIG. 1) and a decryption unit 32. The technique includes encrypting the stream of data at the encryption unit for transferring of an encrypted stream of data from the encryption unit to the decryption unit (see FIG. 1; page 14, lines 13⁺). The encrypting of the stream of data is dynamically varied at the encryption unit by dynamically changing simultaneously multiple encryption parameters of the encryption process, and signaling the dynamic change in encryption parameters to the decryption unit (see page 10, line 24 – page 14, line 12; block 130 of FIG. 2, and page 18, line 22 – page 19, line 17). The dynamically varying of the multiple encryption parameters is responsive to occurrence of a predefined condition in the stream of data (page 18, line 22 – page 19, line 17). Upon receipt of the encrypted data at the decryption unit, the technique includes decrypting the encrypted data, wherein the decrypting accounts for the dynamic varying of the encrypting by the encryption unit using the simultaneously changed, multiple encryption parameters (page 15, line 19 – page 16, line 17).

In further aspects, Appellants' technique includes multiplexing the changed encryption parameters and the encrypted data at a sender prior to transferring thereof to a receiver containing the decryption unit and demultiplexing of the changed encryption parameters and the encrypted data at the receiver (see claims 4 & 31, as well as elements 24 & 30 of FIG. 1, and the supporting description thereof).

Issues

1. Whether claims 1, 2, 5, 7-14, 16-19 and 22-27 were rendered obvious under 35 U.S.C. §103(a) to one of ordinary skill in the art by Jones in view of Nardone and further in view of Leppek;
2. Whether claims 1, 13, 14 and 26 were rendered obvious under 35 U.S.C. §103(a) to one of ordinary skill in the art by Aucsmith in view of Nardone and Leppek;
3. Whether claims 4 and 21 were rendered obvious under 35 U.S.C. §103(a) to one of ordinary skill in the art by Jones in view of Nardone and Leppek, and further in view of Chiariglione;
4. Whether claim 28 was rendered obvious under 35 U.S.C. §103(a) to one of ordinary skill in the art by Warren in view of Nardone, and further in view of Leppek;
5. Whether claims 29, 32 and 34-38 were rendered obvious under 35 U.S.C. §103(a) to one of ordinary skill in the art by Jones in view of Warren, further in view of Nardone and Leppek; and,
6. Whether claim 31 was rendered obvious under 35 U.S.C. §103(a) to one of ordinary skill in the art by Jones, Nardone, Leppek and Chiariglione in view of Warren.

Grouping of Claims

Since each ground of rejection provides a grouping of claims, the following groups of claims are included herein:

- I. Claims 1, 2, 5, 7-14, 16-19 and 22-27
- II. Claims 1, 13, 14 and 26
- III. Claims 4 and 21
- IV. Claim 28
- V. Claims 29, 32 and 34-38
- VI. Claim 31

As understood, the claims of one group of claims do not stand or fall with any other groups of claims. Rather, each group of claims is decided independently of the other groups of claims.

Argument

Group I: Claims 1, 2, 5, 7-14, 16-19 and 22-27

Claims 1, 2, 5, 7-14, 16-19 and 22-27 stand rejected under 35 U.S.C. §103(a) as obvious over Jones in view of Nardone and further in view of Leppek. Reversal of this rejection is respectfully requested.

Advantageously, Appellants' invention provides a new technique for protecting a stream of data to be transferred between an encryption unit and a decryption unit. The technique includes dynamically changing simultaneously multiple encryption parameters used to encrypt the stream of data as the stream of data is passing through the encryption unit. This dynamically changing can occur periodically over time, for example, several times a second, thereby allowing only a small segment of the stream of data to be decoded should the encryption parameters used to encrypt that segment of data be uncovered. This concept of dynamically changing simultaneously multiple encryption parameters as a stream of data is being encrypted is believed to comprise a unique approach from any of the applied art, which typically rely upon definition of a predefined policy for changing the encryption process.

Jones describes an encrypted data transmission system employing means for "randomly" altering the encryption keys. Pseudo-random number generators are employed at both the transmitting and receiving stations to supply identical sequences of encryption keys to a transmitting encoder and receiving decoder. An initial random number seed value is made available to both stations. The random number generators are advanced at times determined by predetermined characteristics of the data being transmitted so that, after transmission has taken place, the common encryption key can be known only to the transmitting and receiving stations.

A careful reading of Jones fails to uncover any teaching or suggestion of Appellants' concept of encrypting a stream of data and during the encryption process dynamically varying encrypting of the stream of data by dynamically changing simultaneously multiple encryption parameters. The Jones encryption approach requires pseudo-random binary sequence generation, and requires seed and mask values arranged at the sender and the receiver. Further, a change in Jones to the encryption process involves changing only an encryption key. The change in the encryption key occurs only at a predefined interval arranged a priori between the sender and the receiver. Jones changes the encryption key only when the counted number of bits or words or "items" matches the arranged interval. The disadvantage of this approach is that synchronization is absolutely essential. Bytes lost during transmission throw off the encryption/decryption process without any chance of recovery. In contrast, Appellants' invention of dynamically varying simultaneously multiple encryption parameters as the stream of data is being encrypted ensures that only a small segment of the encrypted data could be exposed or lost should the encryption parameters used to encrypt that segment become uncovered or lost, respectively.

In addition, Appellants' recited process includes signaling the dynamic change in the encryption parameters from the encryption unit to the decryption unit. A careful reading of Jones fails to uncover any teaching or suggestion that the single encryption key change is signaled to the decryption unit. Rather, the patent teaches otherwise by describing a process which relies upon an a priori agreed upon process. In Jones, the decryption unit knows in advance where the encryption key change is to occur. In contrast, Appellants recite a truly dynamic varying of the encryption process wherein the dynamically changed encryption keys are forwarded from the encryption unit to the decryption unit.

At page 35 of the final Office Action, the Examiner states that Appellants' recited aspect of "signaling the dynamic change in the encryption parameters from the encryption unit to the decryption unit" is taught by Jones at Col. 1, lines 66 to Col. 2, line 7, wherein there is an alleged exchange of random number seed values and interval values between the encryptor and decryptor. Appellants respectfully submit that these lines of Jones disclose an a priori arrangement whereby the seed values and interval values are made available to both the transmitting station and a receiving station. Fig. 1 of Jones clearly shows that the interval

EN998146

number and random number seed are inputs to both stations. The transmitting station does not forward the interval number and seed number to the receiving station. Thus, there is no dynamic signaling of information *per se* from the encryption unit to the decryption unit in Jones. In view of this, Appellants respectfully submit that the final Office Action mischaracterizes the teachings of Jones when asserting those teachings against Appellants' invention as recited in the independent claims presented.

Nardone is cited for allegedly teaching dynamically changing encryption parameters used to encrypt a stream of data (and presumably Appellants' recited concept of dynamically varying the encrypting of the stream by changing simultaneously multiple encryption parameters). This characterization of the teachings of Nardone is respectfully traversed.

Nardone describes a policy based selective encryption of compressed video data. Basic transfer units of compressed video data of a video image are selectively encrypted in Nardone in accordance with an encryption policy to degrade the video image to at least a virtually useless state, i.e., if the selectively encrypted compressed video image were to be rendered without decryption. A careful reading of Nardone fails to uncover any dynamic varying of the encryption parameters as a stream of data is being encrypted within an encryption unit as recited by Appellants. The final Office Action notes that Nardone teaches encrypting of a bit stream taking into account encryption granularity, density and delay. However, Nardone does not describe dynamically varying multiple ones of these encryption parameters simultaneously as the encryption of a stream of data progresses.

Nardone is characterized in the final Office Action as teaching specifying encryption parameters via a policy (i.e., the degree of selective encryption in order to degrade video image). Appellants respectfully submit that Nardone does not expressly describe varying of multiple encryption parameters, let alone simultaneously varying multiple encryption parameters dynamically during the encryption process.

Nardone does teach multiple encryption policies can be provided at authoring time, and does discuss the possibility of changing between policies. However, Appellants respectfully submit that this change between policies merely results in a change in the duty cycle of the

encryption process in Nardone, and does not depend upon or suggest that multiple encryption parameters are changed between the policies. A careful reading of Nardone fails to uncover any teaching or suggestion of such a concept. Notwithstanding this, the final Office Action characterizes the change in encryption policy as somehow equating to a dynamic change in multiple encryption parameters during the encryption process. Appellants respectfully traverse this characterization, and submit that a change between predefined policies in Nardone does not equate to or suggest their recited process for dynamically varying the encrypting of a stream of data at an encryption unit by dynamically changing simultaneously multiple encryption parameters. The result of Nardone is simply a change in the duty cycle of the encryption process. Thus, without hindsight reference to Appellants' claimed invention, it is respectfully submitted that one of ordinary skill in the art would not have read the teachings of Nardone as suggesting that multiple encryption parameters could be simultaneously varied dynamically during the encryption process.

Leppek is cited in the final Office Action for allegedly teaching setting multiple encryption parameters at once. This characterization of the teachings of Leppek is respectfully traversed.

Leppek describes a virtual encryption scheme which combines different encryption operators into a compound-encryption mechanism. The encryption operators in Leppek refer to different encryption processes. Thus, in Leppek, data is first encoded using a first encryption scheme, then the same data is encoded using a second encryption scheme, etc., thereby increasing the entropy of the data to make the encoded data look as random as possible.

In contrast, Appellants recite dynamically changing simultaneously multiple encryption parameters while an encryption unit is encrypting a stream of data. In Appellants' approach, different segments of the stream of data are encrypted using different encryption parameters and there is a dynamic change in the encryption parameters such that multiple encryption parameters simultaneously change from one segment to another segment of the stream of data as the stream of data is passing through the encryption unit and being encrypted. In Leppek, there is a static, sequential application of a number of encryption algorithms or encryption operators to the same

segment of data. Leppek describes encrypting the same data multiple times using different encryption operators (i.e., encryption schemes).

At page 33 of the final Office Action, the Examiner seeks to equate Leppek's teaching of a compound sequence of encryption operators, i.e., the sequential application of encryption algorithms, to Appellants' recited language of simultaneously changing multiple encryption parameters during the dynamically varying of the encrypting of the stream of data. The alleged insight of Leppek is application of multiple encryption operators at once. This conclusion is respectfully traversed. Leppek does not teach the application of multiple encryption operators being applied to the data simultaneously. Rather, Leppek describes a sequential application of encryption algorithms to the same data to increase the entropy of the data. Since Leppek describes a process of sequentially applying different encryption processes to the same data, Appellants respectfully submit that the insight allegedly drawn therefrom is in error.

Additionally, Appellants respectfully submit that one of ordinary skill in the art would not have combined Jones, Nardone and Leppek as proposed in the final Office Action. For example, Jones relies on a fixed policy or fixed sequence for changing a single encryption parameter. Nardone describes a process for varying the duty cycle of an encryption scheme based on predefined policies, and Leppek describes a virtual encryption scheme which combines different encryption processes into a sequential, compound encryption mechanism. None of these references, taken singularly or in combination, suggest Appellants' recited concept of dynamically changing the encryption process by simultaneously changing multiple encryption parameters as a stream of data is being encrypted. Because Appellants' approach does not rely upon any predefined policy, the dynamic change in the multiple encryption parameter is signaled from the encryption unit to the decryption unit. Jones, Nardone, and Leppek do not describe any mechanism for signaling dynamic changes in multiple parameters from an encryption unit to a decryption unit. In this regard, Jones does not describe signaling of encryption parameter changes from the encryption unit to the decryption unit. In Jones, a seed value and interval value are established a priori before an encryption process begins and are provided as inputs to both the encryption unit and the decryption unit (see Fig. 1 of Jones). Since they are provided a priori as

inputs to both units, there is no signaling from the encryption unit to the decryption unit of the simultaneous change of multiple encryption parameters.

For the above reasons, Appellants respectfully submit that their invention as recited in independent claims 1, 14 & 27 would not have been obvious to one of ordinary skill in the art based upon the teachings of Jones, Nardone and Leppek. Therefore, reversal of the obviousness rejection to these claims, as well as to the claims which depend therefrom, is requested.

Group II: Claims 1, 13, 14 and 26

Claims 1, 13, 14 and 26 stand rejected under 35 U.S.C. §103(a) as obvious over Aucsmith in view of Nardone and further in view of Leppek. Reversal of this rejection is requested.

Independent claims 1 & 14 are believed allowable over the combination of Aucsmith, Nardone and Leppek as stated in the final Office Action for the same reasons stated above. The teachings of Aucsmith are similar to those of Jones when applied against the independent claims presented, and are believed distinguishable for the reasons stated above in connection with Jones.

As noted in the final Office Action, Aucsmith teaches generation of an encryption key for each Group Of Pictures (GOP) in a stream of video data. For each GOP, an encryption transformation, parameterized by the encryption key of the GOP, is applied to pictures of the GOP. Appellants respectfully submit that Aucsmith teaches an approach for changing a single encryption parameter between GOPs, and is therefore analogous to the teachings of Jones described above when applied against Appellants' independent claims. Thus, for all of the reasons stated above, Appellants respectfully request reversal of the rejection to the Group II claims based upon the combination of Aucsmith, Nardone and Leppek. Aucsmith, Nardone and Leppek do not individually, or in combination, suggest Appellants' recited process of dynamically varying the encrypting of the stream of data at the encryption unit by dynamically changing simultaneously multiple encryption parameters and signaling the dynamic change in encryption parameters to the decryption unit.

For the above reasons, Appellants respectfully request reversal of the obviousness rejection to the claims of Group II.

Group III: Claims 4 and 21

Claims 4 and 21 stand rejected under 35 U.S.C. §103(a) as obvious over Jones in view of Nardone and Leppek, and further in view of Chiariglione. Reversal of this rejection is respectfully requested.

Dependent claims 4 & 21 are believed allowable for the same reasons as the independent claims from which they directly or ultimately depend, as well as for their own additional characterizations. Chiariglione is cited in the final Office Action for allegedly teaching multiplexing of various information into an encrypted bitstream. Without acquiescing to this characterization, Appellants note that Chiariglione does not teach or suggest the above-noted deficiencies of Jones, Nardone and Leppek when applied against the independent claims presented. Specifically, Chiariglione does not suggest dynamically changing simultaneously multiple encryption parameters used to encrypt a stream of data as the stream of data is passing through an encryption unit. Further, Chiariglione does not teach or suggest signaling these dynamic changes of the multiple parameters from an encryption unit to a decryption unit by multiplexing the changed encryption parameters themselves with the encrypted data for transfer to the decryption unit.

For the above reasons, Appellants respectfully request reversal of the rejection to dependent claims 4 & 21 of Group III based upon the combination of Jones, Nardone, Leppek and Chiariglione.

Group IV: Claim 28

Claim 28 stands rejected under 35 U.S.C. §103(a) as obvious over Warren in view of Nardone, and further in view of Leppek. Reversal of this rejection is also respectfully requested.

Independent claim 28 is allowable over the combination of Warren, Nardone and Leppek for at least the same reasons stated herein above with respect to Jones, Nardone and Leppek.

The final Office Action acknowledges at page 28 that Warren does not teach Appellants' recited characterizations of "dynamically varying the encrypting of a stream of data at the encryption unit by dynamically changing simultaneously multiple encryption parameters ...". Appellants agree. Warren describes an encryption process using a scheme such as Hidden Data Transport (HDT) and Post-Compression Hidden Data Transport (PC-HDT). Warren describes certain advantages of using HDT and PC-HDT algorithms over other encoding technologies, but does not even describe switching between HDT and PC-HDT algorithms dynamically. Thus, Appellants respectfully submit that Warren is less relevant to their claimed invention than the Jones patent described above.

For all of the above reasons, Appellants respectfully request reversal of the obviousness rejection to independent claim 28 based on the teachings of Warren, Nardone and Leppek.

Group V: Claims 29, 32 & 34-38

Claims 29, 32 and 34-38 stand rejected under 35 U.S.C. §103(a) as obvious over Jones in view of Warren, further in view of Nardone and Leppek. Reversal of this rejection is respectfully requested.

Dependent claims 29, 32 and 34-38 are believed allowable over the combination of Jones, Warren, Nardone and Leppek for the same reasons stated herein above for the independent claims from which they directly or ultimately depend, as well as for their own additional characterizations. Warren is not believed to teach or suggest any of the above-noted deficiencies of Jones, Nardone, and Leppek when applied against the independent claims presented herewith. In this regard, please reference Appellants' discussion of the Group I claims and Group IV claims.

For all of the reasons stated above, Appellants respectfully request reversal of the rejection to the claims of Group V based upon the combination of Jones, Warren, Nardone and Leppek.

Group VI: Claim 31

Claim 31 stands rejected under 35 U.S.C. §103(a) as obvious over Jones, Nardone, Leppek and Chiariglione, and further in view of Warren. Reversal of this rejection is respectfully requested.

Dependent claim 31 is believed allowable for the same reasons as independent claim 28 from which it depends, as well as for its own additional characterizations. As noted above in connection with the claims of Group III, Chiariglione is not believed to teach or suggest the noted deficiencies of Jones, Nardone, Leppek, and Warren when applied against Appellants' independent claims, and more specifically, independent claim 28. None of the applied material, taken singularly or in combination, suggest Appellants' dynamic encoding technique which includes dynamically changing simultaneously multiple encryption parameters used to encrypt a stream of data as the stream of data is passing through the encryption unit.

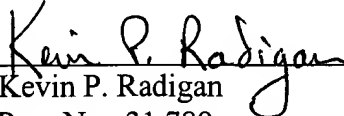
Thus, for the reasons stated above, Appellants respectfully request reversal of the rejection to dependent claim 31 of Group VI based upon the combination of Jones, Warren, Nardone, Leppek and Chiariglione.

Conclusion

Appellants respectfully request reversal of the rejections set forth in the final Office Action. Appellants submit that their claimed invention would not have been rendered obvious by Jones, Warren, Nardone, Leppek, Aucsmith, and Chiariglione. These patents do not, individually or in combination, teach or suggest Appellants' encrypting process which includes dynamically varying the encrypting of the stream of data at the encryption unit by dynamically changing simultaneously multiple encryption parameters, and by signaling the dynamic change and encryption parameters to the decryption unit.

For all the above reasons, Appellants allege error in rejecting their claims as obvious based on the various stated combinations of Jones, Warren, Nardone, Leppek, Aucsmith and Chiariglione. Accordingly, reversal of all rejections is respectfully requested.

Respectfully submitted,


Kevin P. Radigan
Reg. No. 31,789
Attorney for Appellants

Dated: August 23, 2004

HESLIN ROTHENBERG FARLEY & MESITI, P.C.
5 Columbia Circle
Albany, New York 12203
Telephone: (518) 452-5600
Facsimile: (518) 452-5579

Appendix

1. A method for protecting a stream of data to be transferred between an encryption unit and a decryption unit, said method comprising:

encrypting the stream of data at said encryption unit for transferring of said encrypted stream of data from said encryption unit to said decryption unit;
dynamically varying said encrypting of said stream of data at said encryption unit by dynamically changing simultaneously multiple encryption parameters and signaling said dynamic change in encryption parameters to said decryption unit, said dynamically varying of said multiple encryption parameter being responsive to occurrence of a predefined condition in said stream of data;
and

decrypting said encrypted data at the decryption unit, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said dynamically changed, multiple encryption parameters.

2. The method of claim 1, wherein said multiple encryption parameters comprise at least two of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger.

4. The method of claim 2, further comprising multiplexing said changed encryption parameters and said encrypted data at a sender prior to transferring thereof to a receiver containing said decryption unit, and demultiplexing said changed encryption parameters and said encrypted data at said receiver.

5. The method of claim 1, wherein said dynamically varying comprises dynamically varying said multiple encryption parameters based on passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data.

7. The method of claim 1, wherein said stream of data comprises a stream of compressed data, and wherein said method further comprises decompressing said compressed data after said decrypting of said encrypted data by said decryption unit.

8. The method of claim 7, wherein said stream of compressed data comprises one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data.

9. The method of claim 1, further comprising initializing a plurality of encryption parameters based on sensitivity of said stream of data, said plurality of encryption parameters being employed by said encrypting and wherein said changed multiple encryption parameters of said dynamically varying comprise multiple encryption parameters of said plurality of encryption parameters.

10. The method of claim 1, wherein said stream of data comprises a stream of MPEG compressed data, and said method further comprises setting a plurality of encryption parameters for use by said encrypting based upon sensitivity of said stream of MPEG compressed data, and wherein said changed multiple encryption parameters comprise multiple encryption parameters of said plurality of encryption parameters.

11. The method of claim 10, wherein said setting of said plurality of encryption parameters includes establishing at least two of an encryption granularity, an initial encryption key, a density scale, a density, an encryption delay, and a key update data trigger for said stream of MPEG encoded data.

12. The method of claim 1, wherein said encrypting comprises encrypting multiple portions of said data stream, and wherein said dynamically varying comprises dynamically varying said encrypting of said multiple portions of said data stream by changing said multiple encryption parameters for each portion of said multiple portions.

13. The method of claim 1, wherein said dynamically varying comprises dynamically varying said multiple encryption parameters responsive to passage of a predefined number of data bits in said stream of data, or alternatively, responsive to passage of a predefined number of data units in said stream of data, wherein said data units comprise at least one of a program, a sequence, a group of pictures, a picture, a slice, or a macroblock.

14. A system for protecting a stream of data comprising:
an encryption unit and a decryption unit, the encryption unit encrypting the stream of data for transfer to the decryption unit;
means for dynamically varying said encrypting of said stream of data by said encryption unit by dynamically changing simultaneously multiple encryption parameters and signaling said dynamic change in encryption parameters to said decryption unit, said means for dynamically varying being responsive to occurrence of a predefined condition in said stream of data; and
wherein said decryption unit decrypts said encrypted data, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said dynamically changed, multiple encryption parameters.

16. The system of claim 14, wherein said stream of data comprises a stream of digital data.

17. The system of claim 14, wherein said means for dynamically varying comprises means for dynamically varying said multiple encryption parameters based on passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data.

18. The system of claim 14, wherein said encryption unit encrypts multiple portions of the stream of data, and wherein said means for dynamically varying comprises means for changing said multiple encryption parameters for each portion of said multiple portions of said stream of data.

19. The system of claim 14, wherein said multiple encryption parameters comprise at least two of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger.

21. The system of claim 14, further comprising a data multiplexer for multiplexing said changed encryption parameters into said encrypted data for transfer thereof to said decryption unit.

22. The system of claim 14, further comprising means for setting a plurality of encryption parameters based on sensitivity of said stream of data, said plurality of encryption parameters being employed by said encryption unit and wherein said changed multiple encryption parameters comprise encryption parameters of said plurality of encryption parameters.

23. The system of claim 22, wherein said stream of data comprises a stream of compressed data, and wherein said system further comprises a decoder for decompressing said compressed data after decrypting thereof by said decryption unit.

24. The system of claim 23, wherein said stream of compressed data comprises a stream of one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data.

25. The system of claim 22, wherein said means for setting said plurality of encryption parameters includes means for establishing at least two of an encryption granularity, an encryption key, a density scale, a density, an encryption delay, and a key update data trigger.

26. The system of claim 14, wherein said means for dynamically varying comprises means for changing said multiple encryption parameters based on a predefined number of bits being encoded by said encryption unit, or alternatively, based on a predefined number of units being encoded by said encryption unit, said units comprising one of a program, a sequence, a group of pictures, a picture, a slice, or a macroblock.

27. A system for protecting a stream of data to be transferred between a sender and a receiver, said system comprising:

an encryption unit disposed at said sender for encrypting the stream of data prior to transfer to said receiver, said encryption unit being adapted to dynamically vary encrypting of the stream of data by dynamically changing simultaneously multiple encryption parameters based on an occurrence of a predefined condition in said data stream and signaling said change in encryption parameters to said receiver; and

a decryption unit disposed at said receiver for decrypting said encrypted data, said decryption unit being adapted to receive said changed encryption parameters to account for said dynamic varying of said encrypting by said encryption unit using said changed encryption parameters.

28. At least one program storage device readable by a machine, tangibly embodying at least one program of instructions executable by the machine to perform a method for protecting a stream of data to be transferred between an encryption unit and a decryption unit, comprising;

encrypting the stream of data at said encryption unit for transfer thereof to said decryption unit;

dynamically varying said encrypting of said stream of data at said encryption unit by dynamically changing simultaneously multiple encryption parameters and signaling said change in encryption parameters to said decryption unit, wherein said dynamically varying of said multiple encryption parameters is responsive to occurrence of a predefined condition in said stream of data; and

decrypting said encrypted data at the decryption unit, said decrypting accounting for said dynamic varying of said encrypting by said encryption unit using said dynamically changed, multiple encryption parameters.

29. The at least one program storage device of claim 28, wherein said multiple encryption parameters comprise at least two of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger.

31. The at least one program storage device of claim 29, wherein said method further comprises multiplexing said changed encryption parameters and said encrypted data at a sender prior to transferring thereof to a receiver containing said decryption unit, and demultiplexing said changed encryption parameters and said encrypted data at said receiver.

32. The at least one program storage device of claim 28, wherein said dynamically varying comprises dynamically varying said multiple encryption parameters based on passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data.

34. The at least one program storage device of claim 28, wherein said stream of data comprises a stream of compressed data, and wherein said method further comprises decompressing said compressed data after said decrypting of said encrypted data by said decryption unit.

35. The at least one program storage device of claim 34, wherein said stream of compressed data comprises one of MPEG encoded video data, MPEG encoded audio data, and Dolby AC-3 audio data.

36. The at least one program storage device of claim 28, wherein said method further comprises initializing a plurality of encryption parameters based on sensitivity of said stream of data, said plurality of encryption parameters being employed by said encrypting and wherein said

changed multiple encryption parameters of said dynamically varying comprise multiple encryption parameters of said plurality of encryption parameters.

37. The at least one program storage device of claim 28, wherein said stream of data comprises a stream of MPEG compressed data, and said method further comprises setting a plurality of encryption parameters for use by said encrypting based upon sensitivity of said stream of MPEG compressed data, and wherein said changed multiple encryption parameters comprise multiple encryption parameters of said plurality of encryption parameters.

38. The at least one program storage device of claim 37, wherein said setting of said plurality of encryption parameters includes establishing at least two of an encryption granularity, an initial encryption key, a density scale, a density, an encryption delay, and a key update data trigger for said stream of MPEG encoded data.

* * * * *